UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,568	04/11/2006	Dirk Gandolph	PD030108	1348

24498   7590   10/26/2009
Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER
POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 August 2009_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-7 and 9-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-7 and 9-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _11 April 2006_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Remarks

Claims 1-7 and 9-16 are pending.

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/17/2009 has been entered.

Response to Amendment

2.   The most recent amendment, dated 8/17/2009, has incorrectly marked some of the claims. Claim 5 was previously canceled (response dated 1/8/2009), however, previous claim 6 has been marked as claim 5 in the current response. Every claim thereafter is also one claim off. For example, claim 7 of the current claim set states that it is "Previously Presented", however, current claim 7 was previously presented as claim 8 in the prior responses. The first 4 claims are not affected by this issue. This may be rectified by cancelling all current claims and beginning with claim 18 as the first claim (as claim 17's spot is used by current claim 16), or by keeping the first 4 claims, cancelling claims 5-17 (as just discussed, there should be a current claim 17) and putting currently marked claims 5-7 and 9-16 in claims 18 and above, for example. For

purposes of prior art rejection, the Examiner has used the claim numberings as they

appear in the most recent amendment, dated 8/17/2009.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-7 and 9-16 have been considered

but are moot in view of the new ground(s) of rejection.

A brief response is deemed necessary, however, with respect to the arguments

in order to provide sufficient clarity. Regarding the amendment referring to the second

key being different from the first key, this appears to have broad basis in the

specification at the bottom of page 12. However, this basis does not provide any

distinction between a key used to decrypt content on the disk and a key used to decrypt

supplementary data. It states that there may be more than one key on the storage

device, and that at least one key may be used for decryption of supplementary data.

This does not, however, provide basis for the decryption key for supplementary data

and the decryption key for data on the medium to be completely distinct (as in the

previous claim set). The keys may very well overlap and be used for both (e.g. if 3 keys

are used to decrypt the content on the disk, then supplementary data may be decrypted

using the third key while a "first data set" is being decrypted from disk using the first

key). Furthermore, with respect to the arguments regarding keys, Applicant refers to

"decrypting the second data set using a second set of keys different from a first set of

keys". There are no such key sets within the claims, and there does not appear to be

basis for such key sets in the application as originally filed.

Claim Objections

4.   Claims 1, 5, and 10 are objected to because of the following informalities:

-       The preamble of claim 1 refers to "at least two respective device independent electronic decryption key". This was previously fixed to properly refer to plural "keys" instead of a singular "key" since there are multiple keys. This is how the claim has been construed, however, it must be fixed to clearly specify plural keys. Furthermore, it is unclear what these keys are "respective" to. Claim 5 also uses this "respective" language. The word "respective" has been construed as being merely a portion of the name for the keys, wherein each key can be referred to as a "respective device independent electronic decryption key" or "decryption key" with no change in meaning. It is, however, noted, that the device independent and electronic features of these decryption keys are clear.

-       The final limitation of claim 1 refers to "a second of said decryption keys that are different from the first of said decryption keys". However, there is only one "second" of the keys. Therefore, this should read "a second of said decryption keys that is different from the first of said decryption keys". Along these lines, the final limitation of claim 5 refers to "using a different second of said decryption keys". However, there is no second key previously set forth in the claim, so it is unclear how this key can be a different second key. This

has been construed in a like manner as claim 1, in that the second key is

different from the first key, but needs to be clarified.

- Claim 10 recites "the second data set is regarded as authorized if it can be

   decrypted by said decryption key". Multiple keys have been set forth,

   however, within claim 5. The decryption key referred to in claim 10 has been

   construed as the second decryption key of claim 5.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1, 3, 5, 7, 10, 11, 13, 14, and 16 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Kelly (U.S. Patent Application Publication 2003/0072453) in

view of Grooters (U.S. Patent 6,931,593).

Regarding Claim 1,

Kelly discloses a method for decrypting data within a playback

device, the data comprising an encrypted first data set being audio visual

presentation data and an encrypted second data set being audio visual

supplementary data relating to the first data set, wherein the first data set

and at least two respective device independent electronic decryption keys

are stored on a removable prerecorded storage medium (Abstract; and

Paragraphs 28, 31-34, 51, and 63-64; disc keys and title keys stored on

the medium along with a movie or other audiovisual content), and the

second data set is not stored on the removable prerecorded storage

medium but on a second data source and is related to the first data set

(Abstract; and Paragraph 30; additional content items on the server that

are related to the content on the disc), the second data source having a

second data block that is specific to a specified group of removable

storage media and a third data block that is specific to the removable

prerecorded storage medium (Paragraphs 4, 12, 30, and 31; additional

content items including interviews with actors and other participants, live

events, and online games related to the movie comprising, for example,

group content; and additional scenes, different endings, different

soundtracks, etc. comprising, for example, content specific to the

medium), the method comprising the steps of:

Retrieving the first data set and the device independent decryption

keys from the removable storage medium (Abstract; and Paragraphs 34-

36; retrieving the content or encrypted titles and the keys from the disc);

Retrieving the second data set from the second data block of the

second data source (Abstract; and Paragraphs 50 and 57; downloading

additional content items from the server);

Decrypting the first data set using a first of the decryption keys

(Abstract; and Paragraphs 36 and 44; decrypting the encrypted titles); and

Decrypting the second data set using a second of the decryption

keys that is different from the first of the decryption keys (Abstract; and

Paragraphs 50-52, 58-59, and 63-64; as an example, paragraph 63

discusses using the encrypted Disc key as the session key that is used to

encrypt additional content items from the server. This Disc key is not

actually used to decrypt the content itself (the title keys are used to

decrypt the content while the Disc key is used to decrypt the title keys).

Therefore, the encrypted Disc key being used to decrypt additional content

is different from the first key which was used to decrypt the first data set

(encrypted title). In another interpretation, a title key that is not being

currently used to decrypt content on the disk may be used in the

decryption of the additional content, and this would correspond to different

keys being used);

But does not appear to explicitly disclose that the second data

source has a first data block that is public.

Grooters, however, discloses the second data source having a first

data block that is public, a second data block that is specific to a specified

group of removable storage media and a third data block that is specific to

the removable prerecorded storage medium (Column 5, line 61 to Column

6, line 25; Column 7, line 47 to Column 8, line 18; and Column 8, lines 47-

52; additional content is retrieved from the Internet that all may access

(public), such as content regarding shopping, sports, business, etc. from

publicly-accessible websites, such as ESPN.com or concert schedules for

a particular band; further additional content is related to a particular movie

or song, for example based on a DVD or CD that is inserted in the client;

and yet further additional content is related to a group of media, such as

by providing information related action movies or James Bond movies). It

would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the information accessing techniques

of Grooters into the secure content distribution system of Kelly in order to

allow the system to acquire further additional content in a wide variety of

manners (e.g. sub-channels, sub-sub-channels, Internet searching, local

network searching, etc.), thereby allowing each user to access additional

content that is desirable by that user.

Regarding Claim 5,

Claim 5 is an apparatus claim that corresponds to method claim 1

and is rejected for the same reasons.

Regarding Claim 3,

Kelly as modified by Grooters discloses the method of claim 1, in

addition, Kelly discloses detecting whether the removable storage medium

and the second data set are authorized by the same authority, wherein the

second data set is regarded as authorized if it can be decrypted by the

second decryption key (Abstract; and Paragraphs 50-52, 58-59, and 63-64).

Regarding Claim 10,

Claim 10 is an apparatus claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 7,

Kelly as modified by Grooters discloses the method of claim 1, in addition, Kelly discloses that the first electronic decryption key is the only suitable key for decrypting the first data set, and the second decryption key is one of several suitable keys for decrypting the second data set (Abstract; and Paragraphs 36, 44, 51, 58-59, and 63-64; the title keys must be used to decrypt the first data set on the medium, but various keys are able to decrypt the additional content).

Regarding Claim 11,

Claim 11 is an apparatus claim that corresponds to method claim 7 and is rejected for the same reasons.

Regarding Claim 14,

Kelly as modified by Grooters discloses the method of claim 1, in addition, Kelly discloses retrieving a third data set from the third data block, and decrypting the third data set using the second of the decryption keys (Abstract; and Paragraphs 4, 12, 30, 31, 50-52, 58-59, and 63-64).

Regarding Claim 16,

Kelly as modified by Grooters discloses the method of claim 1, in

addition, Kelly discloses that the specified group of removable storage

media comprises media that are provided by a particular provider

(Paragraphs 4, 12, 30, and 31; in order to access the additional content, a

user must own a legitimate specimen of the disc, meaning that the disc

must be a properly produced medium from the provider that creates

and/or distributes that particular disc). Grooters also discloses that the

specified group of removable storage media comprises media that are

provided by a particular provider (Column 7, lines 10-59; providing

channels related to a recording label, which would correlate to a provider,

and extend to movie studios that produce a movie on the disk, for

example).

Regarding Claim 13,

Claim 13 is an apparatus claim that corresponds to method claim

16 and is rejected for the same reasons.

6.   Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kelly in view of Grooters, further in view of Getsin (U.S. Patent 6,529,949).

Regarding Claim 2,

Kelly as modified by Grooters does not explicitly disclose

determining from a plurality of data sets on the second data source a

second data set that refers to the removable storage medium, wherein the
data sets refer to different removable storage media.

Getsin, however, discloses determining from a plurality of data sets
on the second data source a second data set that refers to the removable
storage medium, wherein the data sets refer to different removable
storage media (Column 27, line 56 to Column 29, line 4; showing different
content being provided based on the medium that is currently being
played). It would have been obvious to one of ordinary skill in the art at
the time of applicant's invention to incorporate the remote playback control
system of Getsin into the secure content distribution system of Kelly as
modified by Grooters in order to provide supplemental data for a plurality
of media (e.g. DVDs) on a server, allowing clients to access the data
directed to the media for which the client currently has access (such as
the content being played), while ensuring authentication and authorization
of the user, client, and/or DVD before allowing access to such
supplemental data, and/or to allow the system to access supplemental
data held on the currently playing DVD via such authentication and
authorization processing.

Regarding Claim 6,

Claim 6 is an apparatus claim that corresponds to method claim 2
and is rejected for the same reasons.

7.   Claims 4, 12, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Kelly in view of Grooters, further in view of Qawami (U.S. Patent Application

Publication 2002/0176575).

Regarding Claim 4,

Kelly as modified by Grooters does not explicitly disclose that the

electronic decryption keys are only accessible while a removable

prerecorded storage medium that contains the electronic decryption keys

is readable.

Qawami, however, discloses that the electronic decryption keys are

only accessible while a removable prerecorded storage medium that

contains the electronic decryption keys is readable (Paragraphs 38, 42,

44, 54-58, and 94; the media key is never retained within the device). It

would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the key/content protection techniques

of Qawami into the secure content distribution system of Kelly as modified

by Grooters in order to only provide access to keys while the keys are

being used to decrypt specific data on the disk, and to delete the keys

immediately after use, thereby only storing keys for the amount of time it

takes to decrypt the data, and/or to only provide access to decrypted

content in portions that are rewritten as soon as they are rendered,

thereby increasing security of the keys as well as the content.

Regarding Claim 15,

Kelly as modified by Grooters does not explicitly disclose that only

encrypted data is stored within the player and wherein decrypted data is

only temporarily buffered.

Qawami, however, discloses that only encrypted data is stored

within the player and wherein decrypted data is only temporarily buffered

(Paragraph 55; temporarily storing only currently required portions of

decrypted data). It would have been obvious to one of ordinary skill in the

art at the time of applicant's invention to incorporate the key/content

protection techniques of Qawami into the secure content distribution

system of Kelly as modified by Grooters in order to only provide access to

keys while the keys are being used to decrypt specific data on the disk,

and to delete the keys immediately after use, thereby only storing keys for

the amount of time it takes to decrypt the data, and/or to only provide

access to decrypted content in portions that are rewritten as soon as they

are rendered, thereby increasing security of the keys as well as the

content.

Regarding Claim 12,

Claim 12 is an apparatus claim that corresponds to method claim

15 and is rejected for the same reasons.

8.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Grooters, further in view of Schneier (Schneier, Bruce, "Applied Cryptography", Second Edition, 1996, pp. 1-14.

Kelly as modified by Grooters does not explicitly disclose that the first and second data sets are encrypted using RSA coding.

Schneier, however, discloses that the first and second data sets are encrypted using RSA coding (Pages 6-14). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of Schneier into the secure content distribution system of Kelly as modified by Grooters in order to use an encryption algorithm that is well known, easy to understand and implement, widely used, and secure.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437